STATEMENT OF WORK

Contract Number: **N66001-15-D-0056**
Task Order: **0012**
Tracking Number: **6197-H0018**
Task Order Title: **COMPACFLT Information Assurance Support**
Date: 15 July 2016

1.0 SCOPE

This is a level of effort service to provide Information Assurance and technical support for COMPACFLT N6 accredited systems in order to maintain their Authority To Operate (ATO). The systems involved are the Secured Enterprise Access Tool (SEAT) classified and unclassified instances and the SEAT Unclassified Development Local Area Network (SEAT DEVLAN) under the COMPACFLT Information Technology (IT) Operations requirements for Space and Naval Warfare (SPAWAR) Systems Center Pacific, Pacific C4ISR Department.

1.1 BACKGROUND

COMPACFLT N6 has developed the SEAT systems to provide Single Sign-On (SSO) and centralized user provisioning and authentication for web applications hosted on the SEAT systems. The SEAT Unclassified and Classified systems have valid ATO's and are accredited via the DoD Information Assurance Certification and Accreditation Process (DIACAP). Both systems are due for reaccreditation and transition from DIACAP to Risk Management Framework (RMF) for Assessment & Authorization (A&A). Additionally, the packages need to be updated to include data center relocation, technology refresh of the operating systems and database technology, and the introduction of other operating systems.

The SEAT DELVAN is slated to be migrated into another accredited network. The transition will require some level of IA support to meet the requirements of the new network.

2.0 APPLICABLE DOCUMENTS

In the event of a conflict between the text of the Statement of Work (SOW) and the references cited herein, the text of the SOW shall take precedence. Nothing in the document, however, shall supersede applicable laws and regulations, unless a specific exemption has been obtained. The following documents are for guidance only, except where invoked for a specific section of this SOW.

2.1 Department of Defense Directive 8140.01 (DoDD 8140) Cyberspace Workforce Management

2.2 Department of the Navy (DON) Information Assurance (IA) Workforce Management Manual (SECNAV M-5239.2)

2.3 Department of Defense Instruction 8510.01 (DODI 8510) Risk Management Framework (RMF) for DoD Information Technology (IT)

2.4 Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG)

2.5 OPNAVINST F3300.53C (Series), Navy Antiterrorism Program

2.6 DOD 5220.22-M (Series), National Industrial Security Program Operating Manual (NISPOM)

2.7 National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298

2.8 DOD 5205.02E (Series), DOD Operations Security (OPSEC) Program

2.9 OPNAVINST 3432.1A (Series), DON Operations Security

2.10 SPAWARINST 3432.1 (Series), Operations Security Policy

3.0 REQUIREMENTS

3.1 The contractor shall provide all required administrative support for required for the screening, submission, modification, and validation of Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) or Risk Management Framework (RMF) packages for the SEAT Unclassified and Classified systems and the development of accreditation related documentation for the SEAT DEVLAN.

3.2 The contractor shall maintain SEAT-U and SEAT-C turnover binders as required by N6.

3.3 The contractor shall maintain the accreditation status of SEAT-U and SEAT-C in eMASS by performing quarterly updates or as needed, to update security controls, Plan of Actions and Milestones (POA&M), Risk Assessment Report (RAR), Certification and Accreditation (C&A) plan, and other artifacts as required by the DIACAP or RMF processes.

3.4 The contractor shall review SEAT-U and SEAT-C applicable Security Technical Implementation Guide (STIG) updates to identify updates that need to be addressed to maintain the accreditation status for both systems.

3.5 The contractor shall interpret STIG checklist items and research appropriate remediation or mitigation for those items, test recommendations and work with the system administrators and application developers to ensure the recommendations do not break functionality.

3.6 The contractor shall conduct the annual comprehensive security review effort to ensure that 1/3rd of the STIG checklists are revalidated for SEAT-C and SEAT-U, and that all documentation (policies, procedures, etc.) are kept up to date.

3.7 The contractor shall conduct the annual contingency plan and disaster recovery review for SEAT-U and SEAT-C. Ensure results are documented and recommendations for updates are incorporated into the plans.

3.8 The contractor shall support triennial COMPACFLT Cyber Security Inspections (CSI).

3.9 The contractor shall support SEAT DEVLAN migration to an accredited network.

3.10 The contractor shall obtain and maintain training and/or certification as required by N6 and DoD.

3.11 The following IA workforce categories, levels, training, and certifications are required for contractor personnel under this task order: Information Assurance Manager (IAM) Level I is required, with CompTIA Security+ ce serving as primary qualifying certification.

3.12 The contractor shall ensure that personnel accessing information systems have the proper and current IA certification to perform IA functions in accordance with COMPACFLT's Cyber Security Workforce program, which is aligned to the requirements identified in DoD 8140.01. The contractor shall meet applicable information assurance certification requirements, including (a) DoD-approved IA workforce certifications appropriate for each specified category and level and (b) appropriate operating system training for information assurance technical positions as required by DoD 8140.01. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

3.13 The contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions, reporting current IA certification status and compliance using **CDRL (A002)** Contractor Roster, DI-MGMT-81596.

3.14 The contractor shall complete a Contractor's Progress, Status and Management Report monthly **(CDRL A001)** covering all of the above tasks. The contractor shall immediately notify the Technical Coordinator and the Contracting Officer Representative (COR) if it identifies problems that may negatively impact completion of the tasks in this SOW including schedule, cost, quality and rework issues.

4.0 GOVERNMENT FURNISHED INFORMATION/MATERIAL/PROPERTY

4.1 None.

5.0 CONTACTOR FUNISHED MATERIAL

5.1 None.

6.0 TRAVEL

6.1 None.

7.0 SECURITY

7.1 The work to be performed under this task shall be at the Secret level.

7.2 Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at https://atlevel1.dtic.mil/at/, if experiencing problems accessing this website contact ssc_fortrav@navy.mil.

7.3 As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

7.4 Operations Security: OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or CPI, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

8.0 PLACE OF PERFORMANCE

8.1 Work on this task order will be performed on-site at Pearl Harbor, Hawaii, and SSC Pacific offices.